Ako matematická logika umožnila automatizované usudzovanie

Ján Mazák

FMFI UK Bratislava

Čo je výrok? *Oznamovacia veta*,

- ktorá má pravdivostnú hodnotu.
- ktorej sa dá priradiť pravdivostná hodnota.
- pre ktorú má zmysel otázka na jej platnosť, správnosť, pravdivosť.

Nech x je kladné reálne číslo. Potom $x^2 > 0$.

Predstavme si, že p, q sú výroky.

- Je „p or not p“ výrok?
- Je „p or not q“ výrok?

Ako definovať *jednoduchý výrok*? „Neobsahuje logické spojky.“

- x delí y
- existuje číslo k také, že k je prirodzené a $y = kx$

Hovoríme to isté, lenže raz s logickou spojkou a raz bez.

Pritom ak chceme uchopiť zložitosť výrokov, treba aspoň vedieť určiť, ktoré sú tie najjednoduchšie.

Mimo Zeme žijú niekdajší obyvatelia Atlantídy.

Počet hviezd je nepárny.

Zajtra dva atómy vodíka vytvoria jadro hélia.

Zajtra dva atómy vodíka vytvoria jadro hélia.

Odteraz až navždy každú sekundu dva atómy vodíka vytvoria jadro hélia.

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?
- Aký je význam troch bodiek ako symbolu? Môže byť súčasťou výroku popis algoritmu?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?
- Aký je význam troch bodiek ako symbolu? Môže byť súčasťou výroku popis algoritmu?
- Môže byť výrok nekonečne dlhý?

Bu bayonot emas.

- Znamená „toto nie je výrok“ v uzbečtine. Aký jazyk je prípustný?
- Čo ak má v rôznych jazykoch ten istý reťazec rôzny význam?

Bu bayonot emas.

- Znamená „toto nie je výrok“ v uzbečtine. Aký jazyk je prípustný?
- Čo ak má v rôznych jazykoch ten istý reťazec rôzny význam?
- Môže výrok hovoriť o sebe?
- Môže viesť k paradoxom: Zoberme množinu X všetkých množín, ktoré neobsahujú samé seba. Je veta „X patrí do X“ výrok? Nemôže to byť ani pravda, ani nepravda, pritom to vyzerá ako korektné matematické vyjadrenie.

Chlieb predávajú v potravinách.

Chlieb predávajú v potravinách.

- každý chlieb predávajú len v potravinách a nikde inde
- každé potraviny predávajú aspoň jeden chlieb
- existujú potraviny, ktoré predávajú aspoň jeden chlieb
- existuje druh chleba, ktorý predávajú len v miestnej predajni potravín
- existuje druh chleba, ktorý predávajú v každých potravinách
- ...

Sumarizácia problémov

- Pravdivosť je veľmi ťažké uchopiť.
- Výrok v sebe nesie odkazy na reálny svet, ktoré nesúvisia s logikou a ťažko sa vyhodnocujú.
- Ľudský jazyk je nepresný a nejednoznačný.
- Potrebujeme nejaké obmedzenia na použité symboly a ich prípustné kombinovanie.

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);
- logická štruktúra výroku (spojky, kvantifikátory) bola oddelená od sveta, ktorý výrok popisuje;

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);
- logická štruktúra výroku (spojky, kvantifikátory) bola oddelená od sveta, ktorý výrok popisuje;
- symboly, z ktorých výrok pozostáva, patrili do nejakej fixnej abecedy a ich použitie podliehalo jednoznačným syntaktickým/gramatickým pravidlám.

Jazyk logiky

Konštanty zastupujú konkrétne objekty popisovaného sveta.

Jazyk logiky

Konštanty zastupujú konkrétne objekty popisovaného sveta.

Predikáty zastupujú nejaké vlastnosti popisovaného sveta, logike je úplne jedno, aké vlastnosti to sú.

Jazyk logiky: príklad

Každý človek umrie.	$\forall x \left(C(x) \implies U(x)\right)$
Sokrates je človek.	$C(s)$
Sokrates umrie.	$U(s)$

Konštanty: s
Predikáty: C, U

Jazyk logiky

Formula — postupnosť symbolov s jasne danými pravidlami (dobre uzátvorkovaná, logické spojky majú správny počet operandov, za kvantifikátorom nasleduje premenná atď.).

Jazyk logiky

Formula — postupnosť symbolov s jasne danými pravidlami (dobre uzátvorkovaná, logické spojky majú správny počet operandov, za kvantifikátorom nasleduje premenná atď.).
Príklady formúl:

- $0 = 1$
- $\forall x \; (x \neq 0 \implies x = 1)$
- $\forall x \; \exists y \; [P(x) \wedge Q(x, y)]$
- $P(x) \implies \neg Q(7)$
  — tzv. otvorená formula, zodpovedá výrokovej forme

Jazykov logiky existuje viacero, líšia sa

- konštantami
- predikátmi
- povolenými logickými spojkami (napr. zakážeme ekvivalenciu)
- prítomnosťou kvantifikátorov
- ...

Niektoré obmedzenia (napr. kvantifikátory) majú zásadný vplyv na to, čo možno v jazyku vyjadriť, a následne na algoritmické ťažkosti pri určovaní vlastností formúl.

Pravdivosť formúl

Je $P(\text{alf})$ pravda?

Aby bolo možné skúmať pravdivosť, treba pridať intepretácie pre všetky mimologické symboly.

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).
- Kvantifikované premenné nadobúdajú hodnoty z domény: $\exists x\ P(x)$ vyjadruje, že v D sa nachádza prvok d, pre ktorý platí $P(d)$.

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).
- Kvantifikované premenné nadobúdajú hodnoty z domény: $\exists x\ P(x)$ vyjadruje, že v D sa nachádza prvok d, pre ktorý platí $P(d)$.

Úloha: uvažujme formulu $\forall x\ (x = c_0 \vee x = c_1)$.
Nájdite doménu a interpretáciu konštánt, pre ktoré je táto formula (a) pravdivá, (b) nepravdivá.

Načo je to dobré? Databázy

Databáza: tabuľky, v ktorých sú uložené zoznamy objektov.

Meno	*Rodné číslo*
Ján	1234
Petra	5678
Michal	9876

Táto tabuľka popisuje akýsi predikát P s dvomi argumentmi. Dátové typy určujú doménu, naplnenie tabuliek dátami určuje interpretáciu.

Databázy sa potom pýtame:

„rodné čísla ľudí, ktorí sa volajú Jozef“ $= \{rc \mid P(Jozef, rc)\}$

„rodné čísla všetkých ľudí“ $= \{rc \mid \exists m\ P(m, rc)\}$

Načo je to dobré? Databázy

Databázový systém určuje, ktoré formuly sú povolené.
Čím zložitejšie formuly, tým viac možno vyjadriť, ale ťažšie sa vyhodnocujú.

Aj preto sa dotazy píšu v špeciálnych jazykoch ako SQL, nie v C či Pythone.

Logické vyplývanie

Jedna formula môže byť pravdivá i nepravdivá, závisí od interpretácie predikátov a konštánt.
Zväčša nás nezaujíma vymýšľanie interpretácií, ale vzťahy medzi formulami — logické vyplývanie. Napr. či z pravidiel aritmetiky, popísaných formulou PA, vyplýva tvrdenie F: „súčet dvoch prvočísel je vždy párny“.

Toto sa dá úplne presne definovať: Je pravda, že v každej interpretácii, kde je PA pravdivá, je aj F pravdivá?

Logické vyplývanie

Ak máme konečnú doménu, je ľahké rozhodnúť o vyplývaní:

- vieme vyhodnotiť kvantifikátory, lebo za premennú možno dosadiť len konečne veľa objektov z domény;
- je len konečne veľa možných interpretácií predikátov a stačí všetky vyskúšať.

Lenže typicky máme doménu nekonečnú (napr. reálne čísla) a kvantifikátorov sa nevieme zbaviť, lebo by sme stratili vyjadrovaciu silu jazyka. Preto miesto skúmania pravdivosti robíme dôkazy.

Čo je to dôkaz?

Kľúčová idea: dokazovacie systémy sú mechanické, algoritmické, realizovateľné na počítači bez akýchkoľvek úvah o tom, čo je pravda či pre ktoré interpretácie je formula pravdivá.
Korektnosť a úplnosť.

Čo je to dôkaz?

Príklad dokazovacieho systému: priamy dôkaz. Je to postupnosť formúl, z ktorých každá je axiómou, alebo vzniká aplikáciou pravidla na predchádzajúce formuly. Príklady pravidiel:

- ak v postupnosti máme $A \implies B$ aj A, tak môžeme pripísať B.
- ak v postupnosti máme $A \implies B$ aj $\neg B$, tak môžeme pripísať $\neg A$.

Pravidlá musia byť korektné: pripísaná formula musí logicky vyplývať z predošlých. To zaručí, že čokoľvek, čo dokážeme, je pravda.

Pravidlá musia byť syntaktické: pri aplikácii pravidla sa riadime čisto štruktúrou formuly, nie pravdivosťou ani logickým vyplývaním.

Hilbertov program (1900): nájdime takú sadu axióm (teóriu), že pre každú matem. formulu F možno dokázať F alebo $\neg F$.

Čosi podobne sa podarilo Euklidovi s planimetriou: na základe 5 axióm (v skutočnosti asi 20) dokázal platnosť všetkých podstatných planimetrickych tvrdení známych Grékom.

Gödelova veta o neúplnosti (1930)

Nemožno axiomatizovať ani len aritmetiku. Presnejšie, nemožno nájsť teóriu T, ktorá má zároveň nasledujúce vlastnosti:

- T je prvého rádu a je korektná [ak nie, pravdivosť nebude totožná s dokázateľnosťou],
- z T nevyplýva nepravda [ak by vyplývala, tak z tejto nepravdy už vyplýva čokoľvek, čiže T je nanič],
- T je efektívne axiomatizovateľná [ak by nie, nevieme algoritmicky ani len rozhodnúť, čo je formula či dôkaz],
- T obsahuje aritmetiku (sčítanie, násobenie, prirodzené čísla),
- T je negačne úplná (pre každú formulu vyjadriteľnú v jazyku T máme jej dôkaz alebo vyvrátenie).

Čomu sa venuje logika dnes?

- zúženia prvorádovej logiky (napr. monadická), logika vyššieho rádu
- rôzne výpočtové aspekty (automatické dokazovače, SAT solvery, zložitosť problémov)
- fuzzy logika, modálne logiky (reprezentácia „možno“/„morálne akceptovateľné“/...)
- mnoho teoretických tém, ktorým nerozumiem